UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,274	02/16/2004	Giovanni M. Della-Libera	MS1-1858US	2211

22801 7590 03/17/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
03/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,274	DELLA-LIBERA ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/10/2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-36 and 38-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-36 and 38-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/10/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 01/10/2008. Claims 1-4, 6-36, & 38-48 are pending and have been considered as follows.

Claim Objections

1. Claims 19 & 38 are objected to because of the following informalities:

- Claim 19 line 2 recites the term "when" which should be omitted;
- Claim 38 line 2 recites the term "when" which should be omitted;

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 19 is rejected under 35 U.S.C. 102(e) as being anticipated by Benantar et al. (US-6854056-B1).

Claim 19:

Benantar et al. disclose a computer readable storage medium comprising,

- "computer readable instructions that, when executed by a processor, performs the method of claim 1" (i.e. "The present invention may be implemented on a variety of hardware and software platforms") [column 4 lines 19-20].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4, 6, 8-18, 20-24, 26-36, & 38-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benantar et al. (US-6854056-B1).

Claim 1:

Benantar et al. disclose a method of processing multiple types of security schemes comprising,

- "receiving a message having an associated token" (i.e. "User 302 possesses X.509 digital certificate 304, which is transmitted to an Internet or intranet application 306 that comprises X.509 functionality for processing and using digital certificates") [column 6 lines 35-38];

- "the token is associated with a subject" (i.e. "The entity that receives certificate 304 may be an application, a system, a subsystem, etc. Certificate 304 contains a subject name or subject identifier that identifies user 302 to application 306, which may perform some type of service for user 302") [column 6 lines 38-41];

but, they do not explicitly disclose,

- "authenticating the token by extracting a first claim and a second claim from the token," although they do suggest an identity and associated secret, as recited below;
- "wherein the first and second claims comprise a statement about the subject," although they do suggest host identity mapping, as recited below;
- "grouping the first and second claims into a claim collection by selectively mapping the first claim to the second claim," although they do suggest mapping identities, as recited below;
- "authorizing the first and second claims by mapping them to other claims," although they do suggest verification of identities, as recited below;

however, Benantar et al. do disclose,

- "Host system 410 retrieves the HostID mapping information from the certificate and obtains an identity and associated secret information so that user 402 can be authenticated to various other applications or services within host system 410, such as legacy application 414, using only the presentation of certificate 404" [column 7 lines 16-20];

- "The host identity mapping extension, shown as HostIDMapping in FIG. 6, is a construct that contains: hostName, which identifies the host on which the associated subject identifier is located" [column 7 lines 32-35];
- "map the identity of the certificate holder to a host identity of the certificate holder" [column 8 lines 12-14];
- "Certifying authority 716 verifies the identity of user 702 in some manner and determines whether to issue a digital certificate for user 702" [column 8 lines 48-50];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "authenticating the token by extracting a first claim and a second claim from the token" and "wherein the first and second claims comprise a statement about the subject" and "grouping the first and second claims into a claim collection by selectively mapping the first claim to the second claim" and "authorizing the first and second claims by mapping them to other claims," in the invention as disclosed by Benantar et al. for the purposes of identity mapping.

Claim 2:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "obtaining another claim from the token" (i.e. "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems") [column 7 lines 61-65].

Claim 3:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "rejecting the message as a function of the first claim" [Fig 8c illustrates an authentication of a client based on host identity information and secret information].

Claim 4:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "rejecting the message as a function of the second claim" [Fig 8c illustrates an authentication of a client based on host identity information and secret information].

Claim 6:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "obtaining a resource identifier from the message" [Fig 8c illustrates obtaining host identities and associated secret].

Claim 8:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 6 above, further comprising,

- "the resource identifier comprises a property of the message" [Fig 8c illustrates host identity associated secret].

Claim 9:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "obtaining a resource identifier from the message" [Fig 8c illustrates obtaining host identities and associated secret].

Claim 10:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 9 above, further comprising,

- "the resource identifier comprises a property of the computing system's runtime environment" [Fig 8c illustrates host identity associated secret].

Claim 11:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 9 above, further comprising,

- "a resource corresponding to the resource identifier is stored by the computing system" [Fig 8c illustrates a client being authenticated to additional outside systems].

Claim 12:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "sending a return message to a sender of the message" (i.e. "The certifying authority then returns the certificate to the client (step 834), and the process of generating the certificate is complete") [column 9 lines 61-63];

- "the return message includes information regarding the second claim" (i.e. "The certifying authority encrypts the host identity mapping information using the previously obtained host public key") [column 9 lines 52-54].

Claim 13:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 12 above, further comprising,

- "the information regarding the second claim comprises the second claim" (i.e. "The certifying authority encrypts the host identity mapping information using the previously obtained host public key") [column 9 lines 52-54].

Claim 14:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "obtaining a third claim from the first claim" (i.e. "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems") [column 7 lines 61-65].

Claim 15:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "obtaining a third claim from the second claim" (i.e. "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems") [column 7 lines 61-65].

Claim 16:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "selectively rejecting the first claim" [Fig 8c illustrates authentication of a client based on host identity information and secret information].

Claim 17:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "the token is received out-of-band from the message" (i.e. "The user may then access all applications or systems in which the user has an assigned identity within the distributed data processing system") [column 10 lines 48-51].

Claim 18:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 1 above, further comprising,

- "sending the message, the token and a second token to another entity" (i.e. "The host system then uses the received host identity and secret information to authenticate the certificate holder on another system, subsystem, application, server, etc.") [column 10 lines 13-16];
- "the second token includes information related to the second claim" (i.e. "The host identity mapping extension, shown as HostIDMapping in FIG. 6, is a construct that contains: hostName, which identifies the host on which the associated subject identifier is located") [column 7 lines 32-35].

Claim 20:

Benantar et al. disclose a system configured to process multiple types of security schemes comprising,

- "one or more computer processors" (i.e. "Data processing system 110 contains one or more central processing units (CPUs) 112") [column 3 lines 61-62];
- "one or more computer readable storage media" (i.e. "random access memory (RAM) 114, read-only memory 116") [column 10 lines 62-64];
- "wherein the message has an associated subject" (i.e. "The host identity mapping extension, shown as HostIDMapping in FIG. 6, is a construct that contains: hostName, which identifies the host on which the associated subject identifier is located") [column 7 lines 32-35];

but, they do not explicitly disclose,

- "executable by the one or more computer processors, to store: a first module to extract a first claim and a second claim from a token associated with a message," although they do suggest an identity and associated secret, as recited below;
- "the first and second claims comprise a statement related to the subject," although they do suggest host identity mapping, as recited below;
- "a second module to selectively map the first claim to the second claim," although they do suggest mapping identities, as recited below;

however, Benantar et al. do disclose,

- "Host system 410 retrieves the HostID mapping information from the certificate and obtains an identity and associated secret information so that user 402 can be authenticated to various other applications or services within host system 410, such as legacy application 414, using only the presentation of certificate 404" [column 7 lines 16-20];
- "The host identity mapping extension, shown as HostIDMapping in FIG. 6, is a construct that contains: hostName, which identifies the host on which the associated subject identifier is located" [column 7 lines 32-35];
- "map the identity of the certificate holder to a host identity of the certificate holder" [column 8 lines 12-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "executable by the one or more computer processors, to store: a first module to extract a first claim and a second claim from a token associated with a message"

and "the first and second claims comprise a statement related to the subject" and "a second module to selectively map the first claim to the second claim," in the invention as disclosed by Benantar et al. for the purposes of identity mapping.

Claim 21:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a third module to determine as a function of the first claim whether the message is to be rejected" [Fig 8c illustrates authentication of a client based on host identity information and secret information].

Claim 22:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a third module to determine as a function of the second claim whether the message is to be rejected" [Fig 8c illustrates authentication of a client based on host identity information and secret information].

Claim 23:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a module to form a claim collection that includes the first and second claims" (i.e. "map the identity of the certificate holder to a host identity of the certificate holder") [column 8 lines 12-14].

Claim 24:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a module to selectively obtain a resource identifier from the message" [Fig 8c illustrates obtaining host identities and associated secret].

Claim 26:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 24 above, further comprising,

- "the resource identifier comprises a property of the message" [Fig 8c illustrates host identity associated secret].

Claim 27:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a module to selectively obtain a resource identifier from a computing system in which the first and second modules reside" [Fig 8c obtaining host identities and associated secret].

Claim 28:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 27 above, further comprising,

- "the resource identifier comprises a property of the computing system's runtime environment" [Fig 8c illustrates host identity associated secret].

Claim 29:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 27 above, further comprising,

- "a resource corresponding to the resource identifier is stored by the computing system" [Fig 8c illustrates a client being authenticated to additional outside systems].

Claim 30:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a module to selectively send a return message to a sender of the message" (i.e. "The certifying authority then returns the certificate to the client (step 834), and the process of generating the certificate is complete") [column 9 lines 61-63];
- "the return message includes information regarding the second claim" (i.e. "The certifying authority encrypts the host identity mapping information using the previously obtained host public key") [column 9 lines 52-54].

Claim 31:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 30 above, further comprising,

- "the information regarding the second claim comprises the second claim" (i.e. "The certifying authority encrypts the host identity mapping information using the previously obtained host public key") [column 9 lines 52-54].

Claim 32:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "the second module is to selectively obtain a third claim from the first claim" (i.e. "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems") [column 7 lines 61-65].

Claim 33:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "the second module is to selectively obtain a third claim from the second claim" (i.e. "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems") [column 7 lines 61-65].

Claim 34:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "the second module is to selectively reject the first claim" [Fig 8c illustrates authentication of a client based on host identity information and secret information].

Claim 35:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "the first module is to receive the token out-of-band from the message" (i.e. "The user may then access all applications or systems in which the user has an assigned identity within the distributed data processing system") [column 10 lines 48-51].

Claim 36:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a module to send the message, the token and a second token to another entity" (i.e. "The host system then uses the received host identity and secret information to authenticate the certificate holder on another system, subsystem, application, server, etc.") [column 10 lines 13-16];
- "the second token includes information related to the second claim" (i.e. "The host identity mapping extension, shown as HostIDMapping in FIG. 6, is a construct that contains: hostName, which identifies the host on which the associated subject identifier is located") [column 7 lines 32-35].

Claim 38:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor comprising,

- "receiving a message having an associated token" (i.e. "User 302 possesses X.509 digital certificate 304, which is transmitted to an Internet or intranet application 306 that comprises X.509 functionality for processing and using digital certificates") [column 6 lines 35-38];
- "wherein the token is associated with a subject" (i.e. "The entity that receives certificate 304 may be an application, a system, a subsystem, etc. Certificate 304 contains a subject name or subject identifier that identifies user 302 to application 306, which may perform some type of service for user 302") [column 6 lines 38-41];

but, they do not explicitly disclose,

- "obtaining a first claim and a second claim from the token," although they do suggest an identity and associated secret, as recited below;
- "wherein the first and second claims comprise a statement about the subject," although they do suggest host identity mapping, as recited below;
- "selectively mapping the first claim to the second claim," although they do suggest mapping identities, as recited below;

however, Benantar et al. do disclose,

- "Host system 410 retrieves the HostID mapping information from the certificate and obtains an identity and associated secret information so that user 402 can be authenticated to various other applications or services within host system 410, such as legacy application 414, using only the presentation of certificate 404" [column 7 lines 16-20];
- "The host identity mapping extension, shown as HostIDMapping in FIG. 6, is a construct that contains: hostName, which identifies the host on which the associated subject identifier is located" [column 7 lines 32-35];
- "map the identity of the certificate holder to a host identity of the certificate holder" [column 8 lines 12-14];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a first claim and a second claim from the token" and "the first and second claims comprise a statement related to the subject" and "wherein the first and second claims comprise a statement about the subject" and "selectively mapping the first claim to the second claim," in the invention as disclosed by Benantar et al. for the purposes of mapping identities.

Claim 39:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "rejecting the message as a function of the first claim" [Fig 8c illustrates an authentication of a client based on host identity information and secret information].

Claim 40:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "rejecting the message as a function of the second claim" [Fig 8c illustrates an authentication of a client based on host identity information and secret information].

Claim 41:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "obtaining a resource identifier from the message" [Fig 8c illustrates obtaining host identities and associated secret].

Claim 42:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "obtaining a resource from a computing system reading the machine-readable medium" [Fig 8c illustrates obtaining host identities and associated secret].

Claim 43:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "sending a return message to a sender of the message" (i.e. "The certifying authority then returns the certificate to the client (step 834), and the process of generating the certificate is complete") [column 9 lines 61-63];

- "the return message includes information regarding the second claim" (i.e. "The certifying authority encrypts the host identity mapping information using the previously obtained host public key") [column 9 lines 52-54].

Claim 44:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "obtaining a third claim from the first claim" (i.e. "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems") [column 7 lines 61-65].

Claim 45:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 44 above, further comprising,

- "rejecting the message as a function of the third claim" [Fig 8c illustrates an authentication of a client based on host identity information and secret information].

Claim 46:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "obtaining a third claim from the second claim" (i.e. "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems") [column 7 lines 61-65].

Claim 47:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "selectively rejecting the first claim" [Fig 8c illustrates an authentication of a client based on host identity information and secret information].

Claim 48:

Benantar et al. disclose a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 38 above, further comprising,

- "sending the message, the token and a second token to another entity" (i.e. "The host system then uses the received host identity and secret information to authenticate the certificate holder on another system, subsystem, application, server, etc.") [column 10 lines 13-16];
- "the second token includes information related to the second claim" (i.e. "The host identity mapping extension, shown as HostIDMapping in FIG. 6, is a construct that contains: hostName, which identifies the host on which the associated subject identifier is located") [column 7 lines 32-35].

6. Claims 7 & 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benantar et al. (US-6854056-B1) in view of Clark et al. (XML Path Language).

Claim 7:

Benantar et al. disclose a method of processing multiple types of security schemes, as in Claim 6 above, but do not disclose,

- "obtaining the resource from the message comprises applying an XPath expression," although Clark et al. do suggest the usage of XPath, as recited below;

however, Clark et al. do disclose,

- "XPath uses a compact, non-XML syntax to facilitate use of XPath within URIs and XML attribute values" [page 3];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining the resource from the message comprises applying an XPath expression," in the invention as disclosed by Benantar et al. for the purposes of addressing parts of an XML document…also providing basic facilities for manipulation of strings, numbers and Booleans [Clark et al. page 3].

Claim 25:

Benantar et al. disclose a system configured to process multiple types of security schemes, as in Claim 24 above, but do not disclose,

- "the module to obtain the resource identifier from the message is to selectively apply an XPath expression to obtain the resource identifier," although Clark et al. do suggest the usage of XPath, as recited below;

however, Clark et al. do disclose,

- "XPath uses a compact, non-XML syntax to facilitate use of XPath within URIs and XML attribute values" [page 3];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the module to obtain the resource identifier from the message is to selectively apply an XPath expression to obtain the resource identifier," in the invention as disclosed by Benantar et al. for the purposes of addressing parts of an XML document…also providing basic facilities for manipulation of strings, numbers and Booleans [Clark et al. page 3].

Response to Arguments

7. Applicant's arguments with respect to Claims 1-4, 6-36, & 38-48 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
03/10/2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136